MFT 3.4.0.0 Changelog

EquiSign
76 route de la Demi-Lune
Les Collines de l'arche
92057 Paris La Défense Cedex-France
France
www.equisign.fr

Copyright © 2019 EquiSign. All Rights Reserved.

This product, including its related documentation, is protected by copyright and may be protected by patent.

Restricted Rights. This product, including its associated documentation, is intended to be used exclusively by holders of valid EquiSign licenses for the products documented herein. No part of this document may be reproduced or transmitted, in any form or by any means, without the prior written consent of EquiSign.

Limited Liability. While the utmost precaution has been taken in the preparation of this documentation, EquiSign assumes no responsibility for errors or omissions in this documentation. Information in this document is subject to change without notice and does not represent a guarantee on the part of EquiSign. The documentation is provided "as is" without warranty of merchantability or fitness for a particular purpose. Furthermore, EquiSign does not warrant, guarantee, or make any representations regarding the use, or the results of the use, of the documentation in terms of correctness, accuracy, reliability, or otherwise.

Trademarks and Trade Name. EquiSign® is a registered trademark of EquiSign SAS in the United States and other countries. EquiSign is a trade name of EquiSign SAS in the United States and other countries.

All other brand or product names referred to in this document are registered trademarks, trademarks, service marks, or trade names of their respective owners.

Third-party Reference Documentation. The information contained in this document is not yet part of the standard EquiSign documentation set or is intended to be a reference guide for integrating EquiSign products with third-party software. As such, it is not officially supported or maintained by EquiSign and will not necessarily be updated on the same release schedule as officially supported EquiSign products and their associated documentation.

Pre-release Documentation. The information contained in this document is not yet part of the standard EquiSign documentation set or is intended to be a reference guide for integrating EquiSign products with third-party software. As such, it is not officially supported or maintained by EquiSign and will not necessarily be updated on the same release schedule as officially supported EquiSign products and their associated documentation.

Supplemental Documentation. The information contained in this document is not yet part of the standard EquiSign documentation set or is intended to be a reference guide for integrating EquiSign products with third-party software.

As such, it is not officially supported or maintained by EquiSign and will not necessarily be updated on the same release schedule as officially supported EquiSign products and their associated documentation.

Developer Documentation. The information contained in this document was written for developers by developers as a reference tool. It will not necessarily be updated on the same release schedule as EquiSign products and their associated documentation.

Table of Contents

1. Release Notes for Version 3.4.0.0 3
    1.1. New Features 4
    1.2. Fixed Issues 4
2. Release Notes for Version 3.3.6.6 4
    2.1. New Features 4
    2.2. Fixed Issues 4
3. Release Notes for Version 3.3.6.4 5
    3.1. Fixed Issues 5
4. Release Notes for Version 3.3.6.3 5
    4.1. New Features 5
    4.2. Fixed Issues 5
5. Release Notes for Version 3.3.6.2 5
    5.1. New Features 6
    5.2. Fixed Issues 6
6. Release Notes for Version 3.3.6 6
    6.1. New Features 6
    6.2. Enhancements 6
    6.3. Fixed Issues 6
7. Release Notes for Version 3.3.5 7
    7.1. New Features 7
    7.2. Enhancements 7
    7.3. Fixed Issues 7
8. Release Notes for Version 3.3.4 7
    8.1. New Features 8
    8.2. Enhancements 8
    8.3. Fixed Issues 8
9. Release Notes for Version 3.3.3 8
    9.1. New Features 8
    9.2. Enhancements 8
    9.3. Fixed Issues 9
10. Release Notes for Version 3.3.2 9
    10.1. New Features 9
    10.2. Enhancements 9
    10.3. Fixed Issues 9
11. Release Notes for Version 3.3.1 9
    11.1. New Features 10
    11.2. Enhancements 10
    11.3. Fixed Issues 10
12. Release Notes for Version 3.3.0 10
    12.1. New Features 10
    12.2. Enhancements 11
    12.3. Fixed Issues 11
13. Release Notes for Version 3.2.2 11
    13.1. Fixed Issues 11
14. Release Notes for Version 3.2.1 11
    14.1. Enhancements 12

14.2. Fixed Issues 12
15. Release Notes for Version 3.1.1 12
15.1. New Features and Reasons to Upgrade 13
15.2. Changes 13
15.3. Fixed Issues 13
16. Release Notes for Version 3.1.0 13
16.1. New Features and Reasons to Upgrade 13
16.2. Enhancements 13
16.3. Changes 14
16.4. Fixed Issues 14
17. Release Notes for Version 2.6.1 14
17.1. New Features and Reasons to Upgrade 15
17.2. Enhancements 15
17.3. Changes 15
17.4. Fixed Issues 15
18. Release Notes for Version 2.6.0 15
18.1. New Features and Reasons to Upgrade 15
18.2. Enhancements 17
18.3. Changes 18
18.4. Fixed Issues 18
19. Release Notes for Version 2.5.4 20
19.1. New Features, Improvements, and Changes 20
19.2. Corrections 21
20. Release Notes for Version 2.5.3 21
20.1. New Features, Improvements, and Changes 22
20.2. Corrections 22
21. Release Notes for Version 2.5.2 22
21.1. New Features, Improvements, and Changes 23
21.2. Corrections 23
22. Release Notes for Version 2.5.1 24
22.1. Corrections 24
23. Release Notes for Version 2.5.0 24
23.1. New Features, Improvements, and Changes 24
23.2. Corrections 27
24. Release Notes for Version 2.0.3 29
24.1. Corrections 29
25. Release Notes for Version 2.0.2 29
25.1. Corrections 29
26. Release Notes for Version 2.0.1 30
26.1. Corrections 30
27. Release Notes for Version 2.0.0 30
27.1. New Features, Improvements, and Changes 30
27.2. Corrections 32
28. Release Notes for Version 1.0.0 34
28.1. New Features, Improvements, and Changes 34
28.2. Corrections 34

1. Release Notes for Version 3.4.0.0

Release Date: 05/11/2019

Release Number: 629c7c3

Java OTC Version: 3.9.0

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.6.6 version.

1.1. New Features

New upgrade mechanism: Application updates are now provided in the form of a self-extractable shell script. See the installation guide for more details.

Security: MFT's security has been hardened through both code optimisation and default configuration changes.

1.2. Fixed Issues

Zip encryption: temporary files are now properly deleted.

2. Release Notes for Version 3.3.6.6

Release Date: 26/08/2019

Release Number: 629c7c3

Java OTC Version: 3.7.5

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.6.3 version.

2.1. New Features

RHEL7: MFT now supports RedHat Entreprise (RHEL7) and CentOS 7

At-Rest encryption: MFT now supports transparent file encryption. Files are encrypted and decrypted server-side as they are uploaded/downloaded. The encryption key can either be password-based or wrapped by a key stored in a HSM.

File encryption: Removed legacy EXE encryption method. The two supported methods are now ZIP and 7ZIP.

Deployement: MFT is now distributed as a ISO (base component) and a service pack.

2.2. Fixed Issues

Security: various improvement to security have been made following a security audit. Log file could not be send by email.

User account expiration: performance improvements.

Rest Impersonation: Users connect with their own authentication policy during the impersonation process

Local Setting Management: User with Local Setting Management on a local domain could modify password expiration time

3. Release Notes for Version 3.3.6.4

Release Date: 19/03/19

Release Number:58568ac

Java OTC Version: 3.7.7

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.6.4 version.

3.1. Fixed Issues

Optimization: Clean Inactive User Job is optimized

Security Fixes: MFT is put to the state of the art (upgrade SSL Configuration, XSRF injection)

4. Release Notes for Version 3.3.6.3

Release Date: 20/07/18

Release Number: 629c7c3

Java OTC Version: 3.7.7

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.6.2 version.

4.1. New Features

File Download: we no longer prevent downloading large files on certain OSes/browsers.

CSV user synchronization REST service: the synchronization is now asynchronous, preventing timeouts when processing large files. Additionnal webservices are now available to check the synchronization status.

4.2. Fixed Issues

User account expiration: never-used accounts now expire properly.

5. Release Notes for Version 3.3.6.2

Release Date: 21/12/17

Release Number: 629c7c3

Java OTC Version: 3.7.7

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.6 version.

5.1. New Features

File encryption: When the ZIP encryption method is selected, files are now encrypted as 7ZIP files instead of ZIP files. A lot of users were incorrectly reporting corrupted files, because the default ZIP extractors on both Windows and MacOS do not support AES256-encrypted zip files.

5.2. Fixed Issues

Fixed XSS issue: special characters are now stripped from filenames.

6. Release Notes for Version 3.3.6

Release Date: 2017-08-25

Release Number: r88c3899

Java OTC Version: 3.7.6

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.5 version.

6.1. New Features

N/A

6.2. Enhancements

File encryption: it is now possible to override the default encryption method (ZIP with AES256) at the Domain level. Use this feature if some users are unable to install a compatible Zip extractor on their device.

6.3. Fixed Issues

Encrypted ZIP detection: ZIP and Office files are no longer erroneously detected as encrypted files.

Temporary filename generation: changed the way temporary filenames are generated, to avoid a possible filename collision if different files with the same name are upload simultaneously.

7. Release Notes for Version 3.3.5

Release Date: 2019-11-05

Release Number: 629c7c3

Java OTC Version: 3.7.5

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.4 version.

7.1. New Features

#3030 Download Encrypted Files. All the encrypted files can now downloaded as encrypted zip files.

> **Note**
>
> Thanks to this new feature, it is no longer necessary for MFT to be packaged into an export version, meaning that MFT does not require to be packaged into two versions anymore.

7.2. Enhancements

N/A

7.3. Fixed Issues

#3182 Sender is notified even if the notification checkbox is not checked . Senders of a message are notified even though the notification option is deactivated.

#3186 Bad redirection when the token is invalid. Invalid or expired tokens now redirect to the Docusign website instead of the Idnomic website.

#3187 Notification quand [Quand un message est supprimé] est coché. After deleting a message, a notification was sent even if the option allowing notifications was not set in the preferences. Notifications are now sent only if they are enabled in the preferences.

#3192 A guest cannot download sent files. Guests who used a token to send messages are not able to download the messages and files they have sent.

8. Release Notes for Version 3.3.4

Release Date: 2015-11-18

Release Number: r152202

Java OTC Version: 3.7.4

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.3 version.

8.1. New Features

N/A

8.2. Enhancements

#3158 Comments are now displayed in the audit interface. So far, it was only possible to display the senders and recipients of messages in the audit interface. Now, you can also see messages comments.

8.3. Fixed Issues

- #3156 Signature checkbox is disabled if only one PDF file has been selected. The "PDF Signature" check box is only enabled if at least two PDF documents are attached to the message. It should be activated as soon as one PDF document is attached.
- #3157 Message digest is always the digest of /dev/null. Digests available from the user interface are always the same whatever the message. In addition, digests content represents an empty string.
- #3160 Inactive User Job can be executed on a domain which didn't enable user deactivation.

9. Release Notes for Version 3.3.3

Release Date: 2015-10-02

Release Number: r152201

Java OTC Version: 3.7.3

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.2 version.

9.1. New Features

N/A

9.2. Enhancements

N/A

9.3. Fixed Issues

- #3153 File sending does not respect the sending policy. The maximum size for attachments is not always taken into account by Managed File Transfer.
- #3154 Users whose domain is connected to the same LDAP directory cannot send messages to each other. A registered user cannot send a message to another user when:
  - the recipient is not yet a registered user;
  - both users belong to distinct domains that are connected to the same LDAP directory;
  - the sending policy limits messaging to the current domain.

10. Release Notes for Version 3.3.2

Release Date: 2015-07-30

Release Number: r152198

Java OTC Version: 3.7.1

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.1 version.

10.1. New Features

N/A

10.2. Enhancements

N/A

10.3. Fixed Issues

- #3149 Cannot update Managed File Transfer when using IE 9. The Managed File Transfer update progress bar freezes when using Internet Explorer 9.
- #3150 Cannot send files once Managed File Transfer is installed. It is not possible to send files after a full Managed File Transfer installation is performed.

11. Release Notes for Version 3.3.1

Release Date: 2015-06-03

Release Number: r152198

Java OTC Version: 3.7.1

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.1 version.

11.1. New Features

N/A

11.2. Enhancements

N/A

11.3. Fixed Issues

- #3147 Missing information for OTP authentification. The SMS properties required to implement OTP authentication was not documented so far. For more information, see ???.
- #3143 New authentication policies cannot be created. Creation of a new authentication policy fails because of the lack of OTP authentication scheme related values (SMS Sender and SMS Body) which are mandatory despite the fact that no OTP authentication scheme was used or even created.
- #3142 X-UA compatible forced IE11 to IE9 version. Cannot upload file with Internet Explorer 11.
- #3141 Delivery: No export mode. No export mode is available.

12. Release Notes for Version 3.3.0

Release Date: 2015-04-28

Release Number: r152197

Java OTC Version: 3.7.0

OTC Version: 4.14.5

This section describes the new features, enhancements and corrections provided since the 3.3.0 version.

12.1. New Features

- #3085 OTP authentication plugin. Administrators can now choose to authenticate users through an OTP code sent by SMS. For more information, see the Managed File Transfer Configuration Guide.

- #3084 Password aging. MFT end-users can be forced to change passwords after a certain amount of time. For more information, see the Managed File Transfer Configuration Guide.
- #3067 Automated deletion of inactive users. In version 3.3.0 Administrators can set a period upon which users who have not logged are automatically deactivated. In addition, they can set a grace period upon which inactive users who have not logged yet are automatically removed. For more information, see the Managed File Transfer Configuration Guide.

12.2. Enhancements

- #3023 Adding files to a message does not require the MFT Java Upload Applet anymore. The mechanism to upload and add files to a message now relies on client side JavaScript code.

12.3. Fixed Issues

- #3101 Unsending a message does not correctly remove its temporary files. Cancelling a message now completely removes its temporary files.
- #3056 XSRF Protection is not implemented. Version 3.3.0 of MFT implements XSRF Protection.
- #3078 Cannot activate/deactivate SSL V3. So far, it was not possible to activate/deactivate SSL V3. Version 3.3.0 now provides a new *`enable_sslv3`* network parameter that allows you to activate (*`enable_sslv3=1`*) or deactivate (*`enable_sslv3=0`*) SSL V3 in the `mft.conf` file. Note that, if you activate SSL V3, you must add the *`SSLProtocol -all +TLSv1 +SSLv3`* directive in the `httpd.conf file`. Alternatively, add the *`SSLProtocol -all +TLSv1`* directive when SSL V3 is deactivated.

13. Release Notes for Version 3.2.2

Release Date: 2014-11-04

Release Number: r152191

Java OTC Version: 3.5.0

OTC Version: 4.14.3

This section describes the new features, enhancements and corrections provided since the 3.2.0 version.

13.1. Fixed Issues

- #3020 A fresh MFT 3.2.1 install fails because of a packaging bug (the 3.2.1 upgrade from previous versions works.)

14. Release Notes for Version 3.2.1

Release Date: 2014-1021

Release Number: r152016

Java OTC Version: 3.5.0

OTC Version: 4.14.3

This section describes the new features, enhancements and corrections provided since the 3.2.0 version.

14.1. Enhancements

- #2989 New SAML authentication plugin that does not require a MFT user identification before redirecting to the SAML IdP. When trying to connect to MFT, the user is immediately redirected to the SAML IdP; the SAML user experience is thus smoother.
- #3013 The httpd system execution environment (not to be confused with environment vars passed to CGI scripts) is now configurable by reading environment files whose name matches /opt//mft/var/run/env.d/httpd_*.env

  This is namely useful to load exotic Apache modules such as the CA SiteMinder module.

  If the same key is found several times in the environment files then the corresponding values are appended and separated by the colon symbol ":".

14.2. Fixed Issues

- #3003 File download events are always marked as successful in the audit logs administration console, even if a file download was interrupted by the user.
- #3010 An unexpected error sometimes occurs when attempting to create an upload token.
- #3006 User synchronization with an external LDAP directory becomes slow when there is a large number of users.
- #3014 An unexpected error occurs when attempting to forward a message with an empty subject.
- #3018 A deactivated (or expired) user account receives messages as a registered user instead of receiving them as a guest user as expected, and thus cannot access the messages because she cannot log in MFT.
- #3014 In the user preferences GUI the text relative to notifications received when a message is about to expire displays wrong information.
- #3019 Administration console: it is possible to browse some directories listing static resources such as images or JavaScript files (does not occur for the end-user application).
- #3005 After the Licensing Enforcement removal (see #2983) a symlink is left dangling, which clutters the catalina.out log file with error messages at application startup.

15. Release Notes for Version 3.1.1

Release Date: 2013-05-14

Release Number: r146625

Java OTC Version: 3.3.1

OTC Version: 4.13.1

This section describes the new features, enhancements and corrections provided since the 3.1.0 version.

15.1. New Features and Reasons to Upgrade

N/A

15.2. Changes

N/A

15.3. Fixed Issues

- #2930 A user created through a User Provider cannot authenticate using an email address.
- #2931 When sending a message to a user account created through a User Provided based on File Import, the user is seen as a guest instead of a registered user.

16. Release Notes for Version 3.1.0

Release Date: 2013-02-13

Release Number: r144823

Java OTC Version: 3.3.0

OTC Version: 4.13.1

This section describes the new features, enhancements and corrections provided since the 2.6.1 version.

16.1. New Features and Reasons to Upgrade

- #2388 Message pre-archiving. A pre-archiving policy may be configured and attached to a sending policy. If configured, upon message end of life, message information and files are stored in a directory on the file server. These files are ready to be archived by an external customer-dependant process, typically based on a third-party archiving solution not included with MFT.

16.2. Enhancements

- #1983 Audit log detail enhancements.

16.3. Changes

N/A

16.4. Fixed Issues

- #1368 MIME-type is not set on file download.
- #2480 Messages cannot be forwarded when the sending policy sets encryption as "mandatory" or "optional and suggested."
- #2740 SMTP Connector: Postfix configuration changes prevent local emails from being sent and received.
- #2741 SMTP Connector: Errors are not managed optimally when email size is smaller than the configured minimum size.
- #2742 SMTP Connector: Parsing emails without charset fails.
- #2744 SMTP Connector: Emails starting with characters < or @ cannot be processed.
- #2746 When a sending policy enforces PDF signature, messages cannot be sent without a PDF file attachment.
- #2755 On RHEL 6 in multi-host environments, the nfs-management script uses the portmap service instead of the rpcbind service.
- #2810 With the updateMessage connector operation, the message lifetime may be extended while the sending policy enforces a fixed lifetime.
- #2814 Connector operation listProjects returns the same sending policy for all projects.
- #2821 SMTP Connector: Dependency perl-HTML-Tree is not installed on RHEL 6.
- #2852 The encryption option may be available when forwarding a message after switching between simple and project messages.
- #2868 The "encrypted" parameter in the sendMessage connector operation is not managed correctly if there is a conflict with the sending policy configuration.
- #2884 The SMTP Connector fails when an email does not contain a subject.
- #2888 In the connector sendMessage operation in offline mode, sending encrypted messages with two or more files fails.
- #2890 In the connector sendMessage operation in online mode, sending encrypted messages with two or more files results in the message being malformed.

17. Release Notes for Version 2.6.1

Release Date: 2013-01-04

Release Number: 144043

Java OTC Version: 3.2.1

OTC Version: 4.13.0

This section describes the new features, enhancements and corrections provided since the 2.6.0 version.

17.1. New Features and Reasons to Upgrade

N/A

17.2. Enhancements

N/A

17.3. Changes

N/A

17.4. Fixed Issues

- #2789 Administration console: when searching users belonging to a newly created MFT domain, sometimes no result is found.
- #2790 Administration console: the group management interface of a newly created group is sometimes not correctly displayed, and saving the group may result in an "internal error".

18. Release Notes for Version 2.6.0

Release Date: 2012-12-04

Release Number: r143462

Java OTC Version: 3.2.0

OTC Version: 4.13.0

This section describes the new features, enhancements and corrections provided since the 2.5.4 version.

18.1. New Features and Reasons to Upgrade

- #1267 User Providers. User account creation, update and deletion can now be managed by relying on external datasources. The external user data is mapped to the user entry through a user provider. By configuring a user provider, the administrator decides how the user entry will be created or updated when needed: user properties are computed dynamically depending on the external source data. Currently supported datasources are LDAP (for on-the-fly user creation) and JSON or CSV files (for user synchronization, see #2312). When used with an LDAP datasource, the user provider may be used for authentication and contact suggestions. On-the-fly user creation and update occurs on the following events: first login, first time a user is set or added as message recipient, first time a user is forwarded a message, first time a user is added to a project. User deletion is done through a daily job.

- #2312 File Import for User Providers. A User Provider may be configured with a specific 'File Import' datasource, which enables user synchronization through a file import. The file import may happen either through the administration console (in JSON or CSV format) or through a specific Admin Connector operation (JSON format only). When doing user synchronization, users are created, updated or deleted only when the data file is imported (the file is not retained afterwards).

- #127 LDAP Contact Sources. Contact Sources may now rely on LDAP directories as well as SQL Databases. They are configured through the standard Plugin mechanism and then attached to domains through a contact source. Note that LDAP Contact Sources configuration is not needed when User Providers are configured (see #1267).

- #2038 Message Forward. Sent or received messages may be forwarded to other users, thus avoiding the burden to download/reupload the message files to send it again. The title and comments of a forwarded message may be updated by the sender, but its files cannot be changed. An option in the Sending Policy can be used to allow or forbid the forward of encrypted messages.

- #2221, #2260 SMTP Connector. An SMTP component may be installed. This component receives emails using the SMTP protocol from the organization's mail system, and transfers the messages to MFT. This feature can be used to redirect emails with large attachments to MFT, using the mail system routing mechanisms (for example, MS Exchange transport rules). The component uses the global Impersonation right in order to use any user identity. Note that the SMTP connector requires Postfix as an installation prerequisite.

- #2220 Audit logs segmentation by domain. A new right is available: Local Log Audit. With this right, an administrator is able to view only the logs related to the domains the administrator is entitled to audit. Global logs and logs related to other domains are hidden from the administrator in the audit logs interface.

- #769, #2176 Anti-brute-force system. An anti-brute-force system has been added to MFT to prevent brute force attacks on authentication pages. A user account is temporarily locked when too many authentication attempts fail.

- #2272 SAML Authentication Plugin. MFT 2.6 features a SAML authentication mechanism, based on the standard SAML v2 protocol (see http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.pdf). It can be configured through the "Server Management | Setup | Advanced Settings | Plugins" menu, where detailed online help is available (click on the tooltips).

  MFT acts as a SAML Service Provider (SP), delegating authentication to a SAML Identity Provider (IdP).

  Only SAML authentication is supported in this version; SAML authorization and SAML user account federation are not supported. Hence the following pre-requisites must be respected so that SAML authentication can take place:

  - MFT user accounts must all have been first created in the internal MFT repository (they must pre-exist)

  - MFT user accounts and the IdP user accounts must share a common attribute (usually a UID or the email) so that an MFT account can be mapped to a SAML account.

  Among all of the possible SAML authentication combinations, a subset of the "Web Browser SSO Profile" features has been implemented in MFT 2.6:

  - when sending authentication requests to the IdP, the "HTTP-Redirect" and "POST" bindings are available ("artifacts" are not supported)

  - when receiving authentication responses from the IdP, only the "POST" binding is supported

- authentication requests may be signed
- authentication responses may be signed
- authentication responses may be encrypted. Warning: this feature is experimental
- metadata are not supported; a SP metadata file may be crafted on demand if required by the IdP, but no IdP metadata file is required.

Additional notes:

- MFT does not need a direct network access to the IdP SAML platform; all interactions between MFT and the IdP are performed through the user's browser
- because of technical constraints, the MFT login workflow is a two-step process
- the user is first identified in MFT; the user must provide a UID or email in the MFT login form, but no password
- the user is then redirected to the IdP, where he must authenticate using the IdP's authentication scheme (login/password, X509 client certificate, etc.)

- #2258 In addition to the SOAP protocol, the Admin and Right Connectors can now be used with the REST protocol.
- #2219 RHEL6 64-bit support.
- #2280 CentOS6 support for the OS bundle release.

18.2. Enhancements

- #573 Scheduled job creation and deletion are logged in the audit logs.
- #766 More details are added to the user update audit log when the authentication policy of a user changes.
- #1256 The tuning of the database connection pool can be customized in the MFT configuration file.
- #1403 Custom headers and information are added to notification emails: the event that causes the notification to be sent (X-KEYNECTIS-EVENT), the sender (X-KEYNECTIS-HUMAN-SENDER), the sender domain (X-KEYNECTIS-JOTC-DOMAIN) and the sending software (X-KEYNECTIS-APP).
- #1479 Enhanced the message upload graphical interface for PDF signature selection and tooltip.
- #1527 In addition to the raw text templates, HTML templates are available in the default email notifications.
- #1833 When installing and configuring MFT, the SMTP host may be configured to a custom value instead of the default 'localhost'.
- #1892, #2270 The authentication policy now provides an option to force a user to change their password at the first login.
- #1895 Multi-word filtering and search are available in the end-user interface.
- #1983 Audit logs detail enhancements.

- #1993 The recipient email adresses may be separated by commas or semi-columns.
- #2060 User custom attributes values are recorded in audit logs.
- #2069 Improved tracking information in audit logs.
- #2097 Use of a Blackberry browser is forbidden.
- #2103 Enhanced display performance in the end-user interface when messages have a lot of recipients.
- #2116 RFC3696 compatibility for recipient email authorized characters.
- #2159 file.antivirus.maxFileSize parameter maximum value is raised from 2GB to 64GB.
- #2177 Oracle JRE 7 support for the Java upload applet.
- #2215 In the end-user interface, tooltips are displayed when the mouse hovers over them.
- #2234 Better management of recipient data in the file connectors.
- #2237 Enhanced administration interface performance when managing many domains.
- #2238 The remaining upload time is displayed next to the upload progress bar.
- #2242 Better ClamAV configuration to avoid "false positive" virus detections in some circumstances.
- #2243 The format of the automatic report emails sent by scheduled jobs, quota monitoring or virus monitoring has been normalized.
- #2247 Anti-brute-force system is activated at product installation.
- #2271 Global SMTP settings may be set through the Server Management menu.
- #2273 Support Tool can now be remotely launched on all WebApp servers through the administration console.
- #2276 ClamAV version update.
- #2354 Better ZIP archive file name management when making a ZIP archive with the Java upload applet.
- #2630 The fact that an implicit internal password policy applies when no password policy is explicitly set for a domain is made visible in the configuration interface.

18.3. Changes

- #2208 More permissive browser version compatibility check.
- #2236 Access to file connectors is now granted to all users.
- #2552 The minimal number of users per domain can now be set to "1."

18.4. Fixed Issues

- #1388 General domain configuration and domain notifications may be seen with any local management right. They should only be seen with the "Local Settings Management" local right.

- #1582 When selecting message recipients, contact source suggestions are displayed under a "Server" group.
- #1838 Tabs display in Audit Logs interface does not work with IE9.
- #1984 When exporting the audit logs, actor identifier and realm information are missing.
- #1986 No audit log is created when a message lifetime is extended.
- #1995 Security: upload token value is displayed in the audit logs.
- #1997 MFT upgrade fails if the admin-mft user is not in the MFT domain.
- #1998 A user is always associated with a quota policy, even if no quota policy is displayed in the user edition form.
- #1999 When adding a user quota on the domain, the automatic update of all associated user entries is not correctly handled.
- #2027 SOAP connector: comment with "null" value in the audit logs when a message or an upload token is created without comment.
- #2029 Authentications using a certificate are not recorded in the authentication activity report.
- #2043 Regular increase of the message upload progress bar.
- #2050 Using the character slash "/" in a tag name may have undesired side effects.
- #2051 When an administrator creates a user, policies that do not belong to the selected user domain are unduly displayed if the administrator has rights on them. If an inappropriate policy is selected, the save operation fails.
- #2052 Bad management of domain scopes when editing a user.
- #2053 The IP address of the client and the requested URL are not recorded in the audit logs.
- #2070 Reminder email notifications may be sent an excessive number of times.
- #2071 Strict UNIX access rights on Tomcat configuration files make MFT installation fail.
- #2079 When downloading all message files as a ZIP archive with the "Download All" option, the declared file size is higher than the real file size. On some browsers, download may fail because of this.
- #2101 When the maximum number of users of a domain is reached, it is not possible to edit an existing user entry.
- #2106 Some user preferences settings may avoid notifications to be sent.
- #2125 End-users are not asked to enter their current password when changing passwords.
- #2148 Audit logs import in the audit logs database fails if the audit logs database password contains special characters, namely the pound "#" character.
- #2178, #2179, #2190, #2295, #2399, #2404, #2407, #2412, #2459, #2490 Missing or misleading information in the MFT connectors developer guide.
- #2196 In the createUploadToken connector operation, a "null" comment appears in the email notification when the comment is empty.
- #2198, #2230, #2433, #2440 Some connector operations return invalid error information.

- #2204 A sending policy may be configured with PDF signature even though no signature policy is configured.
- #2218 Audit logs are duplicated when log consolidation is run through the user interface and the scheduled jobs system at the same time.
- #2225 Custom i18n files are not backed up.
- #2244 When configuring email templates whith only email text versions, the HTML body of the sent email is empty.
- #2245 When using the applet to send files under Linux, the files stored in directories accessed through a symbolic link are rejected.
- #2246 It is possible to access the user form of a deleted user.
- #2262 In the searchForUsers connector operation, !domain criterion is not taken into account.
- #2274 Certificate authentication on the connectors fails.
- #2275 In the createUser connector operation, the default domain values are not applied when values are not explicitly provided through the connector.
- #2370 When moving a user from a domain with quotas to a domain without quotas, the user keeps their previous quota policy.
- #2425 When sending an encrypted file, the file size is not correctly displayed.
- #2429 In the sendMessage and getMessages connector operations, the fact that the message is signed or not signed is not provided in the return values.
- #2439 If a message is sent to a project through the sendMessage connector operation, the operation result contains both the "recipient" and "project" keys instead of just "project" as expected.
- #2441 When removing multiple files, the end-user interface does not display a throbber to show that the operation is running.
- #2453 In the listProjects REST operation, the verbose parameter is not optional.
- #2485 The "extend lifetime" button is still available even though the message lifetime is already extended to its maximum value.

19. Release Notes for Version 2.5.4

Release Date: 2012-06-11

Release Number: r139118

Java OTC Version: 2.5.4

This section describes the new features, enhancements, and corrections provided since the 2.5.3 version.

19.1. New Features, Improvements, and Changes

- #2160 The hard limit of the file.antivirus.maxFileSize advanced configuration parameter has been raised to 64GB; it is now possible to scan files up to 64GB provided that the User WebApp has enough memory.

- #2154 Security: HTML elements and attributes that can be used to execute JavaScript are now removed from email templates when they are saved in the Email Templates and MOTD editors.

19.2. Corrections

- #2149 MFT 2.5.3 regression: it is impossible to generate a new license request if MFT has been upgraded from a previous version.
- #2150 MFT 2.5.3 regression: when a domain is created or modified a warning popup is raised.
- #2151 The certificate used to sign the Java applet is expired.
- #2152 Security: the login page is exposed to XSS attacks.
- #2163 Security: using a valid Upload Token, it is possible to download any file of the platform.
- #2167 Security: anyone (no authentication needed) can read the content of the "/opt/opentrust/mft/www/tomcat/" folder by connecting to "https://[machine_hostname]/tomcat" on an MFT server meeting both of the following requirements:
  - the server hosts an MFT Web Server and an MFT User WebApp,
  - the server does not host the MFT Admin WebApp.
- #2181 File Connector: if the sendMessage File Connector method is called without the optional "subject" parameter, it fails with an internal error.
- #2183 MFT 2.5.2 regression: if the sendMessage File Connector method is called without the optional "testrun" parameter, it fails with an internal error.
- #2188 Security: when calling MFT connector methods with both a valid JSESSIONID session cookie but invalid user credentials, the user is still authenticated with the existing session.
- #2191 MFT 2.5.3 regression: an end user without administration right cannot create a project in the user web interface.
- #2197 Security: detail and actor values are not correctly escaped in the Administration Audit logs interface, it could be used in XSS attacks.
- #2200 Security: The clamd with default configuration does not process files whose size is higher than 25MB.
- #2156 Security: In the "Messages" tab of the end user interface, the file name is not correctly escaped in the "Click to download" tooltip, it could be used in XSS attacks.
- #2172 Security: Java stacktraces can be displayed on the end user interface on some errors.
- #2193 Using the sendMessage File Connector method or directly through the end user servlet, a user can still upload messages to projects from which he has been removed.

20. Release Notes for Version 2.5.3

Release Date: 2012-03-29

Release Number: r137468

Java OTC Version: 2.5.3

This section describes the new features, enhancements, and corrections provided since the 2.5.2 version.

20.1. New Features, Improvements, and Changes

- #2118 When used as a company name, "," has been replaced by "KEYNECTIS." Keynectis completed its acquisition of on January 1, 2012.
- #2143 Wibu CodeMeter has been updated to version 4.40 in order to manage licenses not bound to server hardware.
- #2141 An internal hook which can be used to implement a pre-archiving function has been added to the "Message is to be deleted" event.

20.2. Corrections

- #2102 Under certain circumstances, the MessageExpirationNotifications job may send a message reminder email an infinite amount of times.
- #2098 When creating a new user account or editing an already existing user account, a password is requested even if the primary authentication mode of the selected authentication policy is not based on the internal referential.
- #2114 The administration Web interface is slow when dealing with a large amount of profiles, such as hundreds of tags.
- #2121 When an administrator who has only been assigned the "User Management" privilege edits a user account, the displayed user authentication policy is the domain default authentication policy.
- #2093 Starting with MFT 2.5.2, guest user uploads and downloads incorrectly create authentication audit logs in failure state.
- #2122 Starting in MFT 2.5.2, when a user authenticates using the internal reference and exists in a LDAP reference, an authentication failure is indicated on the LDAP reference instead of the internal reference in the corresponding audit log.
- #2123 When a message is sent through an upload token, the recipient is not provided in the corresponding audit log.
- #2131 The Java Applet may stop uploading files due to reduced network or server speeds.
- #2138 The case (upper or lower) used in directory names on Microsoft Windows can cause file selection issues with the Java Applet.

21. Release Notes for Version 2.5.2

Release Date: 2011-11-18

Release Number: r132971

Java OTC Version: 2.5.2

This section describes the new features, enhancements, and corrections provided since the 2.5.1 version.

21.1. New Features, Improvements, and Changes

- #2080 The MFT Web Services now support authentication through JSESSIONID cookie.
- #2081 The MFT File Connector sendMessage method now supports a "dry-run" mode through the "testrun" argument (EXPERIMENTAL feature).
- #2076 The "listProjects" MFT File Connector method now has a verbose argument that allows the caller to get the sending policy details of each project. A "getContext" method has also been added in the File Connector to allow the caller to get various information on the current user context (user firstname, lastname, sending policy, exchange policies, etc...). These two new features are marked as EXPERIMENTAL.

21.2. Corrections

- #1996 The download and upload token values are visible in various audit logs.
- #2018 In the getMessage method of the MFT File Connector, all recipients of a simple message are visible from any recipient.

  #2019 There is no audit logs for the following methods of the MFT Right Connector: addGroupToGroup, addUserToGroup, removeGroupFromGroup, removeUserFromGroup.

  #2021 There is no audit logs for the "getMessage" method of the MFT File Connector.

  #2023 The "getMessage" method of the MFT File Connector does not mark the message as viewed by the user.

  #2025 A message without comment sent through the MFT File connector triggers an error when the message is seen on the user Web interface.

  #2028 Audit logs can contain invalid XML data that make them impossible to process by the logs-manager batch and thus will not visible in the audit log interface.

  #2032 The "Add Recipients" button is available for the message recipients in the message details (user Web interface).

  #2044 In the log detail page of the audit log interface, logs signed by a self-signed certificate are always displayed with a "Wrong Signature".

  #2047 When using the REST (not SOAP) File connector, user credentials are visible in the http_access.log log file and in the audit logs. User credentials can now be given through HTTP headers to workaround this issue. The authentication through HTTP parameters has been kept for backward compatibility.

  #2058 The message encryption functionality does not work anymore in MFT 2.5.1.

  #2035 The getMessage method of the File Connector does not return the message recipients when the message in sent in a project.

  #2054 The message encryption functionnality does not work since MFT 2.5 for messages sent through an upload token.

  #2065 The MFT 2.5 upgrade script installs the codemeter packages on machines where the package is not needed.

  #2067 When creating two tags global to all domains in a row through the Quick Tag Creation, the second tag is local to the first available domain.

#2042 When accessing the Web server in HTTP (because the HTTP access has been enabled), HTTP requests are not logged in the http_plain_access.log file.

22. Release Notes for Version 2.5.1

Release Date: 2011-10-06

Release Number: r131535

Java OTC Version: 2.5.1

This section describes the new features, enhancements and corrections provided since the 2.5.0 version.

22.1. Corrections

- #2039 The PostgreSQL user "mft_readwrite" can access the database server in read and write mode from anywhere without password.

23. Release Notes for Version 2.5.0

Release Date: 2011-07-29

Release Number: r129924

Java OTC Version: 2.5.0

This section describes the new features, enhancements and corrections provided since the 2.0.3 version.

23.1. New Features, Improvements, and Changes

- #1853 A message comment's maximum size has been increased from 2048 to 65536 characters.
- #1852 In the projects list, project members are now sorted alphabetically.
- #1827 In the administration interface, context-sensitive online help tooltips are now accessible by clicking on the help icon, instead of hovering on it.
- #1651 The use of a supported web browser is verified when launching MFT and a warning is displayed when the user connects with a non-officially supported web browser.
- #1552 The third-party ClamAV antivirus application can now be installed through MFT installer.
- #1512 Apache server configuration has been enhanced and tightened for more security.
- #1425 CentOS 5 is now officially supported.

- #1416 The web user interfaces (both End-User and Administration interface) can be accessed via HTTP, in addition to HTTPS. Run /opt/opentrust/sbin/mft-config -x as root on the front-end web server and navigate to "Web Front-end | General configuration" to enable this feature.
- #1415 The mft-config script enables configuration of the "SSLCertificateChainFile" Apache directive in order to set a CA hierarchy for the web server's certificate. This hierarchy is distinct from the one used to authenticate HTTP clients.
- #1408 Handling of sent email headers is improved. Added "Sender:" header and changed configuration semantics to better conform to SenderID requirements.
- #1385 MFT now comes packaged in two versions: an unlimited cryptography strength version, and an export version, limited to weak cryptography strength. The version provided to customers depends on cryptography export laws applicable for the country of purchase.
- #1384 In the activity reports for exchanges, the results can now be grouped by duration or by domain.
- #1382 Mobile Safari is supported on the end-user GUI.
- #1380 The ClamAV daemon is now supported as a built-in anti-virus mechanism. Its use is recommended for performance reasons (it is selected by default on fresh installations).
- #1367 The following attributes can be used either as criteria or return fields when performing user searches with the SOAP Connector: custom1, custom2, custom3, custom4
- #1364 The hash of each uploaded file is available in message details, in email template variables and in the audit logs. Please note that the hash field name in the SOAP sendMessage method has been renamed from md5sum to digest.
- #1363 Add message sender information in FILE_DOWNLOAD audit log.
- #1361 When sending a message to an unknown recipient, the sender may be warned. This behavior of the end-user application is tuned with the userclient.message.confirmUnknownRecipients and userclient.suggestions.highlightUnknownRecipient settings.
- #1357 The "language" user preference is now also used for end-user web interface.
- #1345 In the end-user interface, the recipients suggestion box displays a scrollbar when the size of the suggestion list exceeds the display limit.
- #1336 Enhanced suggestion management when several user details are entered.
- #1302 An OS Bundled version of MFT is available for CentOS (version 5.6).
- #1286 Server-side signature is provided for PDF documents. Signature is configured at the sending policy level and can be enforced, optional, or disabled. The associated signature policy defines the signature configuration:
  - signer certificate to use
  - CA chain inclusion
  - CRL inclusion and verification
  - addition of timestamp
  - addition of visible signature, and watermark
- #1285 For the following languages, if a translation of the software is added, the localized information, such as the date and time, will be displayed in the corresponding locale when

the application is displayed in the language. These languages are Belarusian, Brazilian, Croatian, Czech, Danish, Dutch, German, Greek, Hungarian, Italian, Japanese, Lithuanian, Norwegian, Portuguese, Serbian, Spanish, Swedish, and Ukrainian. For any other language, if a translation of the software is added, the localized information, such as the date and time, will be displayed in English.

- #1270 The diagnostic information file can be generated through the GUI instead of using the "opentrust-support-tool info" command in the command line.
- #1269 Internet Explorer 6 is supported for end-user interface.
- #1265 On Web servers, the mod_proxy configuration of Apache may be tuned by configuring the apache_mod_proxy_common_opts and apache_mod_proxy_balancer_opts in the [network] section of the mft.conf configuration file.
- #1257 An "opentrust-mft-upgrade" script is now available to upgrade MFT.
- #1223 Change of the end-user interface default theme.
- #1213 Web server certificate and audit logs signature certificate private keys can now be imported on the MFT platform via the mft-config script.
- #1209 Added createUsers(), updateUsers(), and deleteUsers() operations to Admin Connector, for batch processing of MFT Users.
- #1208 Command-line interface has been improved. Also, the following scripts have been added: mft-user, mft-tag, mft-system.
- #1194 The list of the servers that are allowed to connect to the MFT database can be restricted. This option is available during the initial configuration.
- #1161 A licence key protection system has been added.
- #1081 During installation, the Java Cryptography Extension is automatically installed on the provided JRE (except in the export MFT version)
- #832 Upload form content is no longer reset when switching between the main "Messages", "Search", and "Send" tabs.
- #781 Enhanced display of upload token state.
- #643 When using X.509 certification authentication with the Java Applet, uploads may fail and certificate selection popups may appear repeatedly. In such a case, the "apache_ssl_enable_insecure_renegotiation" parameter in the "[network]" section should be set to 1. This, however, has a security cost:
  - the client certificate is requested by Apache only for the login URL "/connect"
  - SSLInsecureRenegotiation is "on"
  - on the Tomcat Java side the client certificate is not validated for each user request
- #550 Duration of antivirus scan and file encryption is logged.
- #537 Email notification origin (Return-Path, From and Sender headers) can now be configured per domain.
- #517 Auto-complete suggestions now use a cache mechanism so that the end-user interface only queries the server when necessary.
- #373, #121 Contact groups overhaul : a contact group is made up of contacts, who can be registered users, guest users from the adress book, or guest users who are not yet in the

address book. In the latter case, the guests are automatically added as contacts in the address book.

- #290 The default choice of languages in the GUI is now limited and can be extended through the i18n.langs.additional parameter.
- #195 A scheduled job that checks the inconsistencies between the database and the filesystem has been added. The job either sends a warning email to the administrator, or fixes the issues itself, depending on the batch.dbFilesystemCheck.autoCorrect parameter value.
- #36 The user account expiration job behavior has changed: a user is now disabled for a configurable amount of time and then removed.
- OTC #367 The MD5 cipher is no longer accepted in the Apache configuration.

23.2. Corrections

- #1960 When a message's comment contains line breaks, those are not respected in the notification email HTML form.
- #1917 Inactive or expired users are still considered as registered users when set as recipient of a new message. They should be considered guest users.
- #1688 Reminder emails are still sent after at least one of the message files has been downloaded more than once.
- #1554 On Windows, files whose names use non-Latin characters (such as Cyrillic or Chinese characters) cannot be decrypted.
- #1534 Message filtering in end-user interface does not work with address book contact firstname or lastname.
- #1452 Custom themes are not applied on upload and download token web interface.
- #1418 An internal error may occur when performing file filtering upon uploading a message with the Java applet.
- #1406 When using the HTTP upload mode and uploading a group of files as an archive, the hash associated with the archive is not correct.
- #1393 A message sent to self does not appear in the list of received messages.
- #1381 The User Authentication Management right improperly grants the right to edit the tags of a user.
- #1378 Exchange rules are not correctly enforced when sending messages using the File Connector.
- #1377 Java applet sometimes may not be loaded on Internet Explorer.
- #1374 Not providing the 'comment' parameter to the 'sendMessage' operation on the File REST Connector causes an internal error.
- #1360 A password contaning non-Latin characters (such as Cyrillic or Chinese characters) does not work even if the password policy allows these special characters.
- #1356 A file named with non-ASCII character is altered when it is uploaded.
- #1351 Tomcat temporary files directory is not correctly cleared after upgrade.

- #1312 Filenames with UTF-8 characters are not correctly handled at download step or when using encryption.
- #1310 In the end-user interface, auto-complete suggestions are not displayed in the alphabetical order.
- #1308 With Internet Explorer 7 and 8, upload errors are sometimes badly handled.
- #1301 The Local Settings Management right on a domain does not allow to download the files from a local or global theme.
- #1284 Tomcat logfile is not rotated.
- #1283 On Microsoft Windows, the file extension of a decrypted file is removed if the suggested decrypted file name is changed during the decryption process.
- #1282 In the email template editor, if the HTML template is removed then empty emails are sent.
- #1281 Accented characters are not properly displayed in HTML emails.
- #1273 If the parameter of the field "Warning Threshold" is modified, the value is re-initialized at 50 which is the default value when the policy is saved.
- #1259 Some Apache default settings are not tuned for MFT.
- #1251 When the Administration webapp and the User webapp are launched at the same time, the default configuration properties may be created twice.
- #1250 SOAP connector getGroupMembers operation provides results the principal is not authorized to obtain.
- #1246 Tomcat stops processing requests after a few days of use and needs to be restarted.
- #1237 An administrator with the single right "Local Settings Management" with privilege "assign" or "assign_inh" on a specific domain cannot see the configuration of this domain.
- #1233 With Internet Explorer 9, the applet fails to upload a message if subject or comment fields are left empty.
- #1204 The installer command line fails if an unknown option is provided.
- #1201 The Exchange Policies menu is not displayed to an Administrator with the local Profile Management execution right.
- #1200 Password change option is improperly displayed in the end-user interface if the user is not authenticated through the internal authentication scheme.
- #1171 The User Authentication Management right improperly grants the right to create a new user.
- #1115 A local administrator can change the scope of a tag from global to local, through the SOAP connector.
- #1023 After a large upload using the Java applet on Internet Explorer 7, the applet may no longer work afterward.
- #906 An administrator can remove the user's password or leave the user's password unset if a user's authentication policy contains the internal authentication scheme.
- #846 For any modification of a user's profile, a password change notification is sent.

- #682 An orphan project cannot be deleted.
- #680 The browser's back and forward buttons are not handled correctly in the administration interface.
- #656 User Reports and Activity Reports CSV export fails when using Internet Explorer.
- OTC #358 In audit logs, the infinite scroll does not work with Google Chrome.
- OTC #254 In the "trust-management" CLI script, some errors are not correctly indicated.

24. Release Notes for Version 2.0.3

Release Date: 2011-05-17

Release Number: r127359

Java OTC Version: 2.0.3

This section describes the corrections provided in the 2.0.3 version.

24.1. Corrections

- #1394 LDAP delegated authentication: a user may authenticate with any password when the LDAP connection type is SSL or TLS

25. Release Notes for Version 2.0.2

Release Date: 2011-03-30

Release Number: r124943

Java OTC Version: 2.0.2

This section describes the corrections provided in the 2.0.2 version.

25.1. Corrections

- #1320 Database connection pool exhaustion
- #1322 Rights Management: if group "A" is a manager of group "B" then a member of group "A" can not see the group management menu entry
- #1325 Rights Management: the "Exchange Policies" menu entry is not displayed to a user who has only the "Local Settings Management" right
- #1326 Rights Management: the "Local Settings Management" right allows the creation of LDAP Directory Connections
- #1333 When editing a domain with local administration rights, selected policies in the "General" tab can mismatch the effective selected policies
- #1242 The OTC version is not correctly displayed in the audit interface

- #1323 Non-ascii characters in email HTML templates are not correctly displayed in HTML emails
- #1324 In the "Preferences" tab, the "Click to change your password" link is displayed when the user is not logged using the internal MFT repository
- #1340 The request duplicate action icon is missing in the audit interface

26. Release Notes for Version 2.0.1

Release Date: 2011-01-26

Release Number: r122244

Java OTC Version: 2.0.0

This section describes the corrections provided in the 2.0.1 version.

26.1. Corrections

- #1241 Fixed issue: user authentication fails in some circumstances
- #1243 Fixed issue: the audit log interface cannot be used with Firefox 3.5.16, 3.6.13 and above versions.
- #1244 The command line "mft-diag version" now returns correct information.

27. Release Notes for Version 2.0.0

Release Date: 2010-12-07

Release Number: r122285

Java OTC Version: 2.0.0

This section describes the significant features and corrections introduced in the 2.0.0 version.

27.1. New Features, Improvements, and Changes

- #342 #516 #677 #701 #851 #892 MFT is now a packaged application, with a streamlined installation process and utility/maintenance scripts.
- #756 File Connector. This connector (with SOAP and REST interfaces) allows for management of messages and upload tokens (list/update/delete + send files)
- #757 #807 Activity Reports. Gives synthesized information on the platform's usage.
- #758 File Filtering Policy. Configurable policy can restrict what type of files can be exchanged.
- #760 Audit Logs signature is officially supported.
- #828 Specific MFT domains can be blacklisted on a per machine basis.

- #259 MFT encryption feature now supports encryption of files bigger than 2GB.
- #661 User privileges for sending messages, managing projects, and creating upload tokens are now handled though a single "Exchange Policy."
- #751 Users who attempt to access MFT with an unsupported browser are redirected to a page that explains why they cannot access the application and displays a list of supported browsers.
- #363 Default policies can be defined on a per domain basis, for easy user creation.
- #382 #740 #761 #1017 Various improvements to audit logs: more information is audited, improved error logs handling.
- #718 A user can now reset his password without the help of an administrator (optional feature).
- #728 #735 Guest recipients may be limited in number and guest downloads availability may be limited in time (once downloaded).
- #767 User Management Right has been split: management of authentication-related user information now requires a new User Authentication Management right.
- #960 Creation of identical users (uid or email) on different MFT domains is now forbidden by default.
- #1136 Improved robustness of XHR requests. This should (mostly) alleviate 12019 type errors and some kinds of smartcard authentication errors.
- #285 #518 Improved themes support: login page is now customizable and custom footers can be set.
- #301 Users can now delete incoming messages.
- #662 Project creation is now a discrete privilege. The user's exchange rule for project members management is always applied to project members management *only*. When delegating project management to a third-party user, the third-party user's exchange rule applies and dictates what members he can manage.
- #663 #1129 Various improvements to Users Audit: new search criteria and results, new CSV download defaults.
- #730 User tags can now be managed using the Admin Connector.
- #244 #378 #384 #592 #733 #734 #810 #822 #827 Various improvements to end-user interface.
- #741 The number of users that can be created on a particular MFT domain can now be limited.
- #219 #221 #743 #744 #777 #860 #886 #949 #1017 Various improvements to notifications: separation into categories, new notification events, new variables.
- #870 Improved messages search performance.
- #390 The action triggered by a file validation error event is now configurable (do nothing, send mail to admin contact, or send mail to tech contact).
- #553 User UID syntax can be enforced on a per domain basis (using a regular expression).
- #755 Administrators can now generate a random password through the user information panel. The generated passwords respect the configured password policy.

- #674 When an MFT domain quota is enabled, the current domain quota usage can be reviewed on the domain information page.

27.2. Corrections

- #513 Fixed condition where the Apache HTTP server mod_proxy would break and begin serving random pages.
- #96 #284 #362 #414 #482 #502 #543 #568 #593 #688 #693 #709 #721 #722 #724 #847 Fixed various cosmetic and user interface issues in both the Admin console and the end-user interface.
- #704 Fixed handling of access URLs in notification emails, in multi-URL context. URLs can now be set up on a per MFT domain, with an option to use a standard access URL for guests.
- #713 Fixed performance of various database requests.
- #829 #866 [IE7] Fixed condition where the "please wait" throbber would not disappear. This was caused by a bad handling of the error in the client application.
- #411 Fixed various issues that occurred when a user opened an authenticated session and an upload token session simultaneously, with the same browser.
- #598 #759 Fixed various issues related to quota configuration and display.
- #619 When "Application/Login Customization" settings are changed, "Application/Setup" will now reload automatically when accessed, to reflect the changes.
- #634 A PostgreSQL database restart no longer requires a Tomcat server restart.
- #646 Adding a user to a group one does not manage is no longer possible through the Admin Connector.
- #659 Fixed condition where password policy configuration was not correctly tested.
- #669 Fixed various bugs that occurred when uploading large files (serveral gigabytes) using the Java applet.
- #684 When loading the Java applet, there should not be any security warning related to publisher "Adrian Buerki."
- #691 Fixed security issue where an administrator could search for users of MFT domains he does not have access to.
- #694 Fixed security issue where identification credentials entered on the login page would not be processed prior to being used in database requests.
- #705 Fixed condition where a displayed message expiration date value would be wrong in message listing (real expiration date + 30 days).
- #711 Fixed miscalculation of an MFT domain occupied storage space.
- #725 #726 Fixed condition where audit logs related to authentication would contain false or incomplete information.
- #710 #871 Fixed handling of language used in notifications (Address Book contacts' language is now correctly saved and taken into account).
- #921 #999 Fixed incorrect behaviour of email auto-complete when the exchange rule would restrict the auto-completion.

- #932 Fixed annoying display of multiple "PIN Code entry" windows when accessing MFT with smartcard-based X509 authentication.
- #986 Fixed "custom domains" setting in Exchange Rules, where it would not be possible to remove an MFT domain from the authorized domains list.
- #989 Fixed "custom domains" auto-completion setting in Exchange Rules, where validation would fail even if the selected domains are a correct subset of the "custom domains" exchanges setting.
- #16 When an upload fails (for any reason), existing fields (subject, comments, lifetime, etc.) are now retained.
- #152 #153 Java applet now works on Safari.
- #403 Added firstname to message search criteria.
- #645 Fixed internal error in Right Connector's #getGroupMember method when the requester had no right on users who are members of the group.
- #649 Fixed security issue in Right Connector where a user could list groups he should not be allowed to view.
- #670 [IE7] Fixed condition where a warning "This page contains both secure and non-secure items" message would be incorrectly displayed by the browser.
- #673 Fixed handling of upload cancellation by users, where an error log could be generated.
- #689 Ensure that form validation buttons cannot be clicked more than once.
- #702 The upload mode (standard HTTP / applet) is now retained between uploads.
- #706 Fixed internal error message display when accessing MFT with an invalid upload token.
- #742 [USER_PASSWORD] and [USER_EXPIRATION_DATE] are now replaced by an empty string in email templates, when they are not available.
- #749 Built-in jobs can no longer be renamed or deleted.
- #787 [IE] [Safari] [Chrome] Fixed and improved handling of drop-down menus with "option groups."
- #797 Fixed "Automatically Add Recipients" preferences setting where the option would not be taken into account.
- #833 Fixed condition where the MFT Administrator would received an email each hour when a user notification would fail during a "MessageExpirationAlarmJob" run.
- #386 When the user was authenticated with a non-interactive (X509, SSO...) scheme, the "sign out" link is only available if a logout URL property was set.
- #317 #404 #410 #690 #692 Various fixes related to the rights management interface.
- #456 When the Java applet is not loaded (for example, when the user refused to trust it), an error message is displayed and the upload mode is set back to standard HTTP.
- #788 Fixed XSS security issue where user entered data (in contacts, projects...) would be interpreted as HTML when displayed in the interface.
- #86 User search results are now sorted by lastname|firstname|uid.
- #509 Fixed bad handling of upload errors. All errors should now be caught and correctly rewrapped for client consumption.

28. Release Notes for Version 1.0.0

Release Date: 2010-07-27

Release Number: r116915

Java OTC Version: 1.0.0

This section describes the significant features introduced in the 1.0.0 version.

28.1. New Features, Improvements, and Changes

- First release.

28.2. Corrections

- Not applicable.